UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/080,865	02/21/2002	Ross W. Callon	JNP-0159	9630

44987 7590 11/16/2005

HARRITY & SNYDER, LLP
11240 WAPLES MILL ROAD
SUITE 300
FAIRFAX, VA 22030

EXAMINER	
DELGADO, MICHAEL A	
ART UNIT	**PAPER NUMBER**
2144	

DATE MAILED: 11/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/080,865	CALLON, ROSS W.	
	Examiner	Art Unit	
	Michael S. A. Delgado	2144	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-64* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-64* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/22/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-6, 8-17, 20-28, 32-39, 41-48 and 50-51 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Application Publication No. 2002/0101819 by Goldstone.

In claim 1, Goldstone teaches about a system for detecting and responding to an attack, comprising (Fig 4):

a first device "firewall (20)" attached to a network and configured to detect an attack based on received traffic, create attack information, and forward the attack information to the network (Paragraph 42, lines 1-12); and

a second device " ISP Router (50)" configured to receive the attack information and detect particular traffic based on the attack information (Paragraph 42, lines 1-12).

In claim 2, Goldstone teaches about a system of claim 1, wherein the first device comprises a firewall filter (Paragraph 42, lines 1-12).

In claim 3, Goldstone teaches about a system of claim t, wherein the first device comprises:

a filter device configured to perform stateful filtering (Paragraph 12, lines 1-17) (Paragraph 20, lines 1-7) (Paragraph 42, lines 1-12).

In claim 4, Goldstone teaches about a system of claim 1, wherein the first device comprises:

a packet generating element configured to generate a packet that include the attack information (Paragraph 2, lines 1-7) (Paragraph 42, lines 1-12).

In claim 5, Goldstone teaches about a system of claim 1, wherein the second device comprises a router (Paragraph 42, lines 1-12).

In claim 6, Goldstone teaches about a system of claim 1, wherein the first device uses a distributed routing protocol for sending the attack information (Paragraph 43, lines 1-11).

In claim 8, Goldstone teaches about a system of claim 1, wherein the first device uses one of one of a markup language or hypertext protocol or a network management protocol to send the attack information (Paragraph 42, lines 1-12). (Communication 130 between site router and ISP router has to the access list can only be done using a network management protocol)

In claim 9, Goldstone teaches about a system of claim 1, wherein the second device forwards the attack information to other devices (Fig 4, 130) (Paragraph 42, lines 1-12) (Paragraph 44, lines 1-7).

In claim 10, Goldstone teaches about a system of claim 1, wherein the second device configures a filter based on the attack information (Paragraph 42, lines 1-12) (Paragraph 43, lines 1-11). (router access list is used to realize the filter)

In claim 11, Goldstone teaches about a system of claim 1, wherein the second device uses the attack information for a predetermined amount of time (Paragraph 46, lines 1-8).

In claim 12, Goldstone teaches about a system of claim 1, wherein the second device rate limits the particular traffic (Paragraph 45, lines 1-16).

In claim 13, Goldstone teaches about a system of claim 1, wherein the second device counts the particular traffic (Paragraph 29, lines 1-6). (To determine that a DOS attack has ended, there has to be a reduction in the amount of ill accesses, which cannot be done without a counting function).

In claim 14, Goldstone teaches about a method of detecting and responding to an attack, comprising (Fig 4):

detecting an attack at a first device based on incoming traffic (Paragraph 42, lines 1-12);

generating attack information defining characteristics of the attack (Paragraph 42, lines 1-12);

sending the attack information to a second device in a network (Paragraph 42, lines 1-12);

detecting traffic at the second device based on the attack information (Paragraph 42, lines 1-12).

In claim 15, Goldstone teaches about a method of claim 14, including:

configuring the first device to detect traffic based on the detected attack (Paragraph 42, lines 1-12).

In claim 16, Goldstone teaches about a method of claim 14, wherein the sending includes: sending a packet that includes the attack information (Paragraph 42, lines 1-12).

In claim 17, Goldstone teaches about a method of claim 14, wherein the sending includes:

sending the attack information using a distributed routing protocol (Paragraph 43, lines 1-11).

In claim 20, Goldstone teaches about a method of claim 14, further including:

sending the attack information from the second device to another device (Fig 4,130) (Paragraph 42, lines 1-12).

In claim 21, Goldstone teaches about a method of claim 14, further including:

monitoring the attack at the second device (Paragraph 43, lines 1-11). (The blocking process is done by monitoring for the attacker IP address.)

In claim 22, Goldstone teaches about a method of claim 14, further including:

detecting traffic based on the attack information for a particular period of time (Paragraph 46, lines 1-8).

In claim 23, Goldstone teaches about a method of claim 14, further including:

rate limiting traffic that matches attack characteristics defined in the attack information (Paragraph 45, lines 1-16).

In claim 24, Goldstone teaches about a method of claim 14, wherein the sending includes:

sending the attack information using one of a markup language or hypertext protocol (Paragraph 1, lines 1-7).

In claim 25, Goldstone teaches about a device for detecting an attack, comprising (Fig 4, 20):

an attack detection element configured to detect an attack in incoming traffic (Paragraph 42, lines 1-12);

an attack information generator (function that update access list) configured to generate attack information defining characteristics of the attack (Paragraph 12, lines 1-16) (Paragraph 42, lines 1-12); and

a transmitting element configured to transmit the attack information to a device on a network (Paragraph 42, lines 1-12).

In claim 26, Goldstone teaches about a device of claim 25, further comprising:

a filter element configured to filter incoming traffic and forward filter information to the attack detection element (Paragraph 20, lines 1-7) (Paragraph 42, lines 1-12).

In claim 27, Goldstone teaches about a device of claim 26, wherein the attack information generator is further configured to send attack information to the filter element (Paragraph 42, lines 1-12).

In claim 28, Goldstone teaches about a device of claim 25, wherein the transmitting element is further configured to transmit the attack information using a distributed routing protocol (Paragraph 43, lines 1-11).

In claim 32, Goldstone teaches about a device of claim 25, wherein the attack is a denial of service attack (Paragraph 25, lines 1-5).

In claim 33, Goldstone teaches about a method of detecting an attack, comprising (Paragraph 42, lines 1-12):

monitoring incoming traffic at a first device to detect an attack (Paragraph 42, lines 1-12);

generating attack information defining characteristics of the attack (Paragraph 42, lines 1-12); and

transmitting the attack information to a second device via a network (Paragraph 42, lines 1-12).

In claim 34, Goldstone teaches about a method of claim 33, wherein the attack is a denial of service attack (Paragraph 25, lines 1-5).

In claim 35, Goldstone teaches about a method of claim 33, wherein the monitoring includes:

using information from a filter to detect the attack (Paragraph 19, lines 1-10) (Paragraph 42, lines 1-12).

In claim 36, Goldstone teaches about a method of claim 33, wherein the generating includes:

sending attack information to a filter for configuring the filter based on the attack (Paragraph 19, lines 1-10) (Paragraph 41, lines 8-14).

In claim 37, Goldstone teaches about a method of claim 33, further including:

performing stateful filtering on incoming traffic (Paragraph 12, lines 1-17) (Paragraph 20, lines 1-7) (Paragraph 42, lines 1-12).

In claim 38, Goldstone teaches about a method of claim 33, wherein the transmitting includes:

sending the attack information in a packet (Paragraph 2, lines 1-6) (Paragraph 42, lines 1-12).

In claim 39, Goldstone teaches about a method of claim 33, wherein the transmitting includes:

sending the attack information using a distributed routing protocol (Paragraph 43, lines 1-11).

In claim 41, Goldstone teaches about a method of claim 33, wherein the transmitting includes:

sending the attack information using a markup language protocol or a hypertext protocol (Paragraph 1, lines 1-7).

42. The method of claim 33, wherein the transmitting includes:

sending the attack information in a secure format.

In claim 43, Goldstone teaches about a device for responding to an attack, comprising:

a receiver configured to receive attack information from a first device that sent the attack information (Paragraph 42, lines 1-12); and

a configuration element configured to configure a second device based on the received attack information (Paragraph 42, lines 1-12).

In claim 44, Goldstone teaches about a device of claim 43, further including:

a transmitting element for transmitting the attack information to another device via a network connection (Paragraph 42, lines 1-12) (Paragraph 44, lines 1-7).

In claim 45, Goldstone teaches about a device of claim 43, wherein the configuration element comprises:

a filter (Paragraph 20, lines 1-7) (Paragraph 41, lines 8-14); and

an attack configuration generator (Paragraph 42, lines 1-12).

In claim 46, Goldstone teaches about a device of claim 43, wherein the configuration element is further configured to configure the second device based on filter information (Paragraph 42, lines 1-12) (Paragraph 43, lines 1-11).

In claim 47, Goldstone teaches about a device of claim 43, wherein the configuration element is further configured to unconfigure the second device after a predetermined period of time after configuring based on the attack information (Paragraph 46, lines 1-8).

In claim 48, Goldstone teaches about a device of claim 43, wherein the second device comprises a router (Paragraph 42, lines 1-12).

In claim 50, Goldstone teaches about a device of claim 43, wherein the configuration element is further configured to detect particular traffic based on the attack information (Paragraph 19, lines 1-11) (Paragraph 41, lines 8-14).

In claim 51, Goldstone teaches about a device of claim 43, wherein the configuration element is further configured to monitor traffic and send monitoring results to the first device (Paragraph 19, lines 1-11) (Paragraph 41, lines 8-14).

Claims 52-57 and 59-64 are rejected under 35 U.S.C. 102(e) as being anticipated by US 2002/0032854 by Chen et al.

In claim 52, Chen teaches about a method of responding to an attack, comprising:

receiving attack information from a first device (Fig 2, 102) attached to a network (Paragraph 45, lines 1-24) ;

configuring a second device (Fig 2, 106) based on the received attack information (Paragraph 45, lines 1-24); and

detecting and discarding traffic at the second device based on the received attack information (Paragraph 45, lines 1-24).

In claim 53,Chen teaches about a method of claim 52, wherein the configuring includes:

generating configuration information based on the attack information and filter information (Paragraph 45, lines 1-24).

In claim 54, Chen teaches about a method of claim 52, wherein the configuring includes:

configuring a filter based on the received attack information (Paragraph 45, lines 1-24).

In claim 55, Chen teaches about a method of claim 52, further including:

sending the attack information to another device (Fig 2, 107) via a network connection (Paragraph 45, lines 1-24).

In claim 56, Chen teaches about a method of claim 52, further including:

monitoring traffic at the second device (Paragraph 45, lines 1-24); and

sending monitoring results "history log" to the first device (Paragraph 45, lines 1-24).

In claim 57, Chen teaches about a method of claim 52, further including:

authenticating the received attack information (Paragraph 14, lines 1-19) (Paragraph 45, lines 1-24).

In claim 59, Chen teaches about a method of claim 52, wherein the second device is a router (Paragraph 45, lines 1-24).

In claim 60, Chen teaches about a method of claim 52, wherein the first device "edge router" is a firewall.

In claim 61, Chen teaches about a method for responding to an attack, comprising:

receiving attack information at a central management system (Fig 2, 101) from a first device via a network (Paragraph 44, lines 1-6);

managing a response to the attack at the central management system (Paragraph 45, lines 1-24).

In claim 62, Chen teaches about a method of claim 61, wherein the managing includes: sending the attack information to other devices via a network (Paragraph 45, lines 1-24).

In claim 63, Chen teaches about a method of claim 61, wherein the managing includes:

receiving attack-related information "history log" from other devices via a network (Paragraph 45, lines 1-24); and

communicating to the first device based on the attack-related information (Paragraph 45, lines 1-24).

In claim 64, Chen teaches about a method of claim 61, wherein the managing includes:

collecting information related to the attack information (Paragraph 47, lines 1-11).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 7, 18, 29 and 40 rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Application Publication No. 2002/0101819 by Goldstone in view of US Patent Application Publication No. 2003/0039245 by Khosravi et al.

In claims 7, 18, 29 and 40, Goldstone teaches the limitation as to a router transferring access lists information (Filter information) to another router (Fig 4, 130) (Paragraph 42, lines 1-12) (Paragraph 44, lines 1-7) but does not explicitly teach about using a link state routing protocol.

The Link state protocol is a well-known standard protocol that is used in router-to-router communication as is evident from Khosravi disclosure (Paragraph 52, lines 1-15).

It would have been obvious at the time of the invention for some one of ordinary skill to use a link state routing protocol as an alternative to the routing protocol of Goldstone.

Claims 19, 30-31, 49 and 58 rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Application Publication No. 2002/0101819 by Goldstone and US 2002/0032854 by Chen et al in view of US Patent Application Publication No. 2002/0016926 by Nguyen et al.

Goldstone and Chen teaches about the problem of being attack by a malicious attacker and the need to communicate information about the attack to upstream routers (abstract). Nguyen teaches about an improve method of communication between routers using tunneling which prevent unauthorized access (Paragraph 63, lines 1-14) (Paragraph 96, lines 1-12).

When under the scenario of being attack, it is crucial that the steps that are taken to avoid being shut down, be protected from the attacker. The encryption approach of Nguyen guarantees that the information that is exchange between the different entities is only between authorized entities.

It would have been obvious for some one of ordinary skill at the time of the invention to improve on the method of Goldstone and Chen by using the encryption scheme of Khosravi to insure that the information that is being transmitted to recovery from an attack is from an authorized source and not the attacker.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent Application no. US 2003/0065948 by Wilkes, teaches about identifying potential intruders on a server.

US Patent Application no. US 2002/0157020 by Royer, teaches about firewall for protecting electronic commerce databases from malicious hackers.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael S. A. Delgado whose telephone number is (571) 272-3926. The examiner can normally be reached on 7.30 AM - 5.30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923

. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Wm. C. Vaughn

WILLIAM C. VAUGHN, JR.
PRIMARY EXAMINER